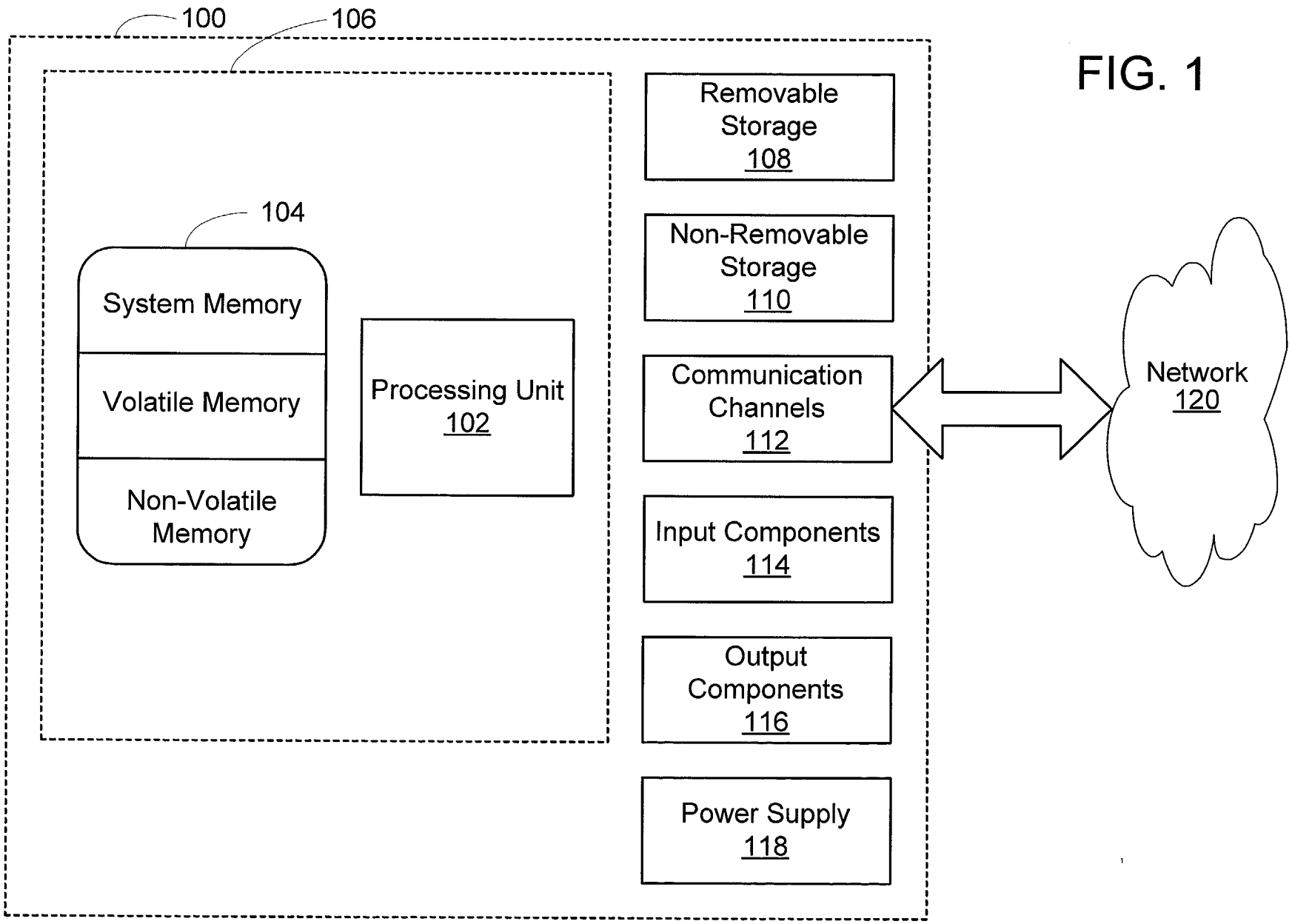

100
106
104
System Memory
Volatile Memory
Non-Volatile Memory
Processing Unit
102
Removable Storage
108
Non-Removable Storage
110
Communication Channels
112
Input Components
114
Output Components
116
Power Supply
118
Network
120

FIG. 1

FIG. 2

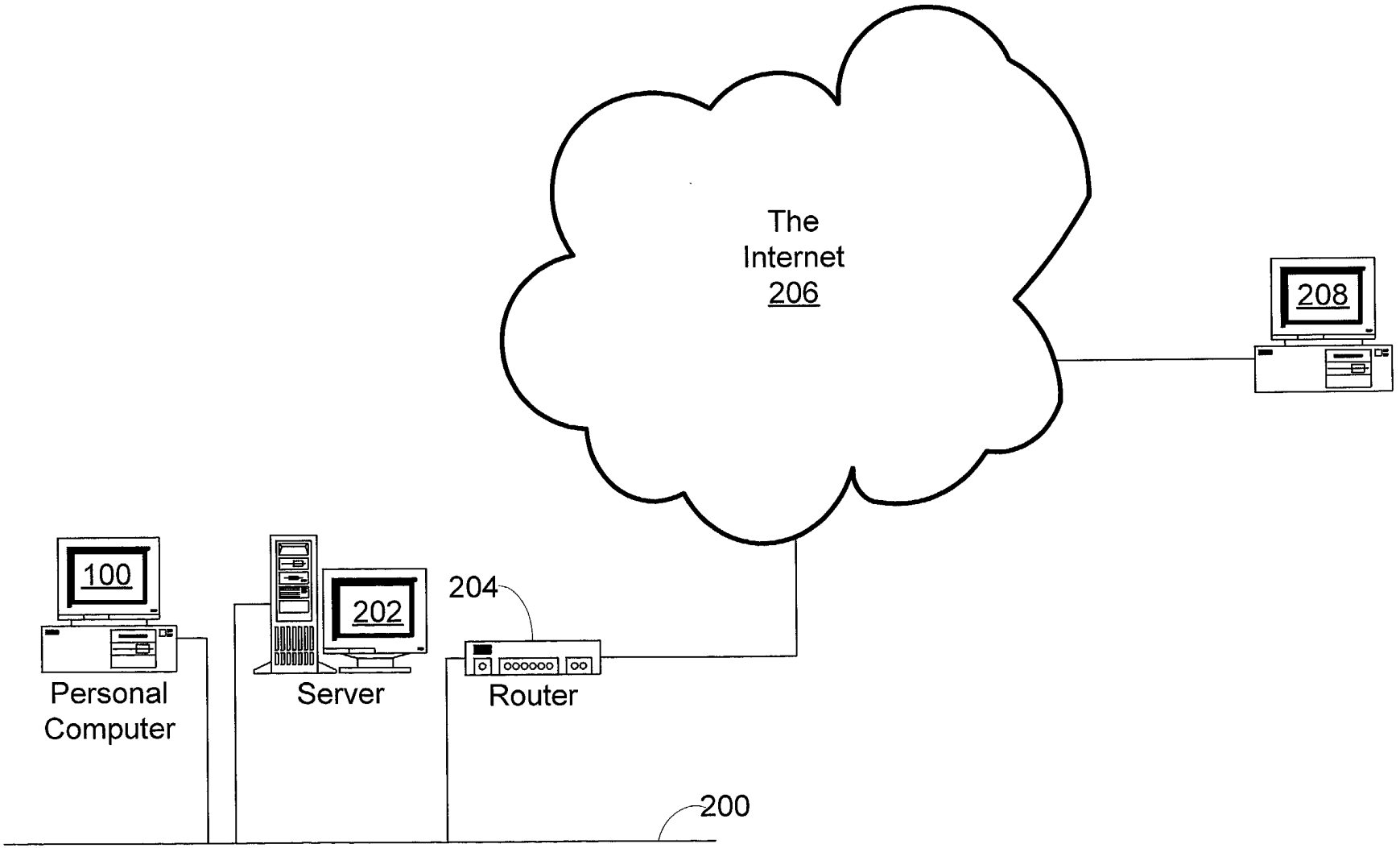
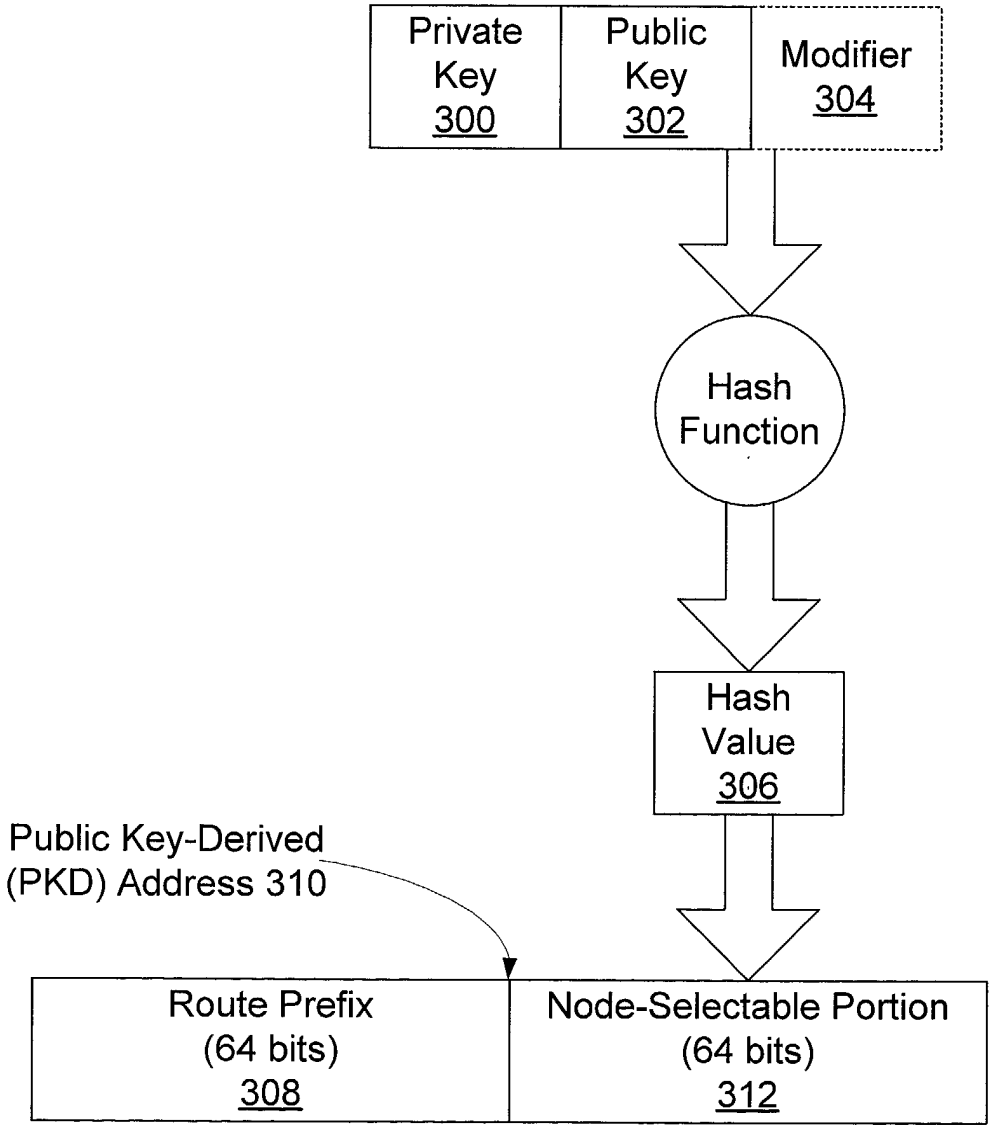

The
Internet
206
208
100
202
204
Personal
Computer
Server
Router
200

FIG. 3


Private Key 300
Public Key 302
Modifier 304
Hash Function
Hash Value 306
Public Key-Derived (PKD) Address 310
Route Prefix (64 bits) 308
Node-Selectable Portion (64 bits) 312

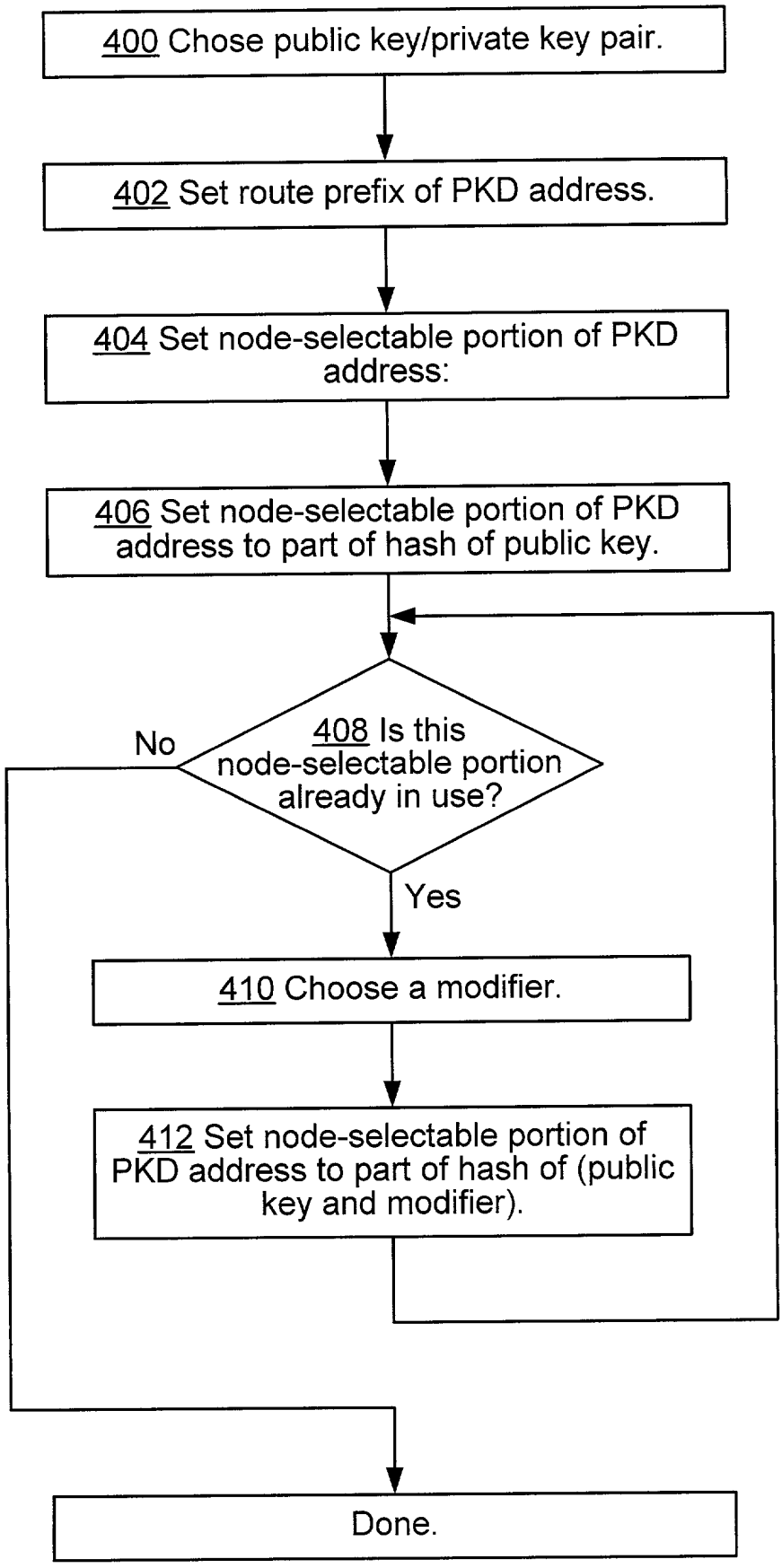

400 Chose public key/private key pair.
402 Set route prefix of PKD address.
404 Set node-selectable portion of PKD address:
406 Set node-selectable portion of PKD address to part of hash of public key.
408 Is this node-selectable portion already in use?
No
Yes
410 Choose a modifier.
412 Set node-selectable portion of PKD address to part of hash of (public key and modifier).
Done.

FIG. 4

FIG. 5

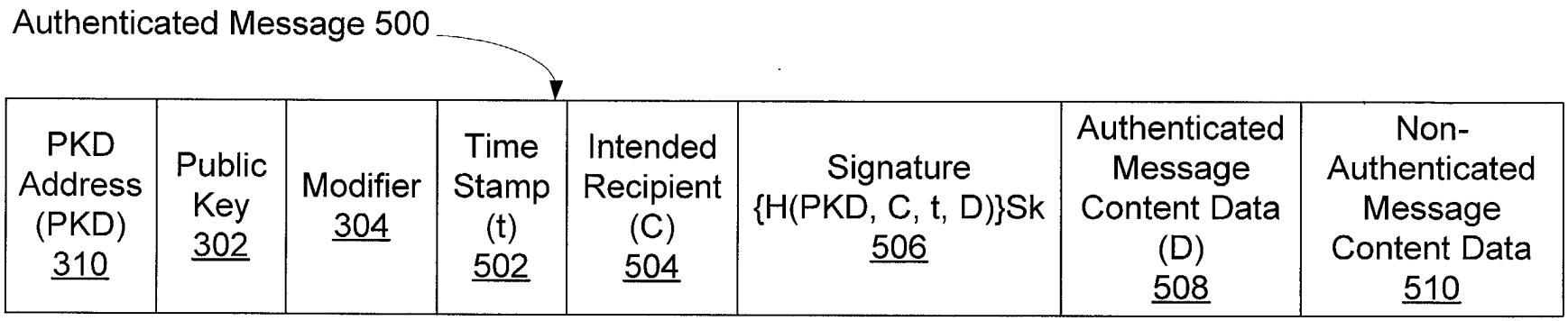

Authenticated Message 500
PKD Address (PKD) 310
Public Key 302
Modifier 304
Time Stamp (t) 502
Intended Recipient (C) 504
Signature {H(PKD, C, t, D)}Sk 506
Authenticated Message Content Data (D) 508
Non-Authenticated Message Content Data 510

FIG. 6

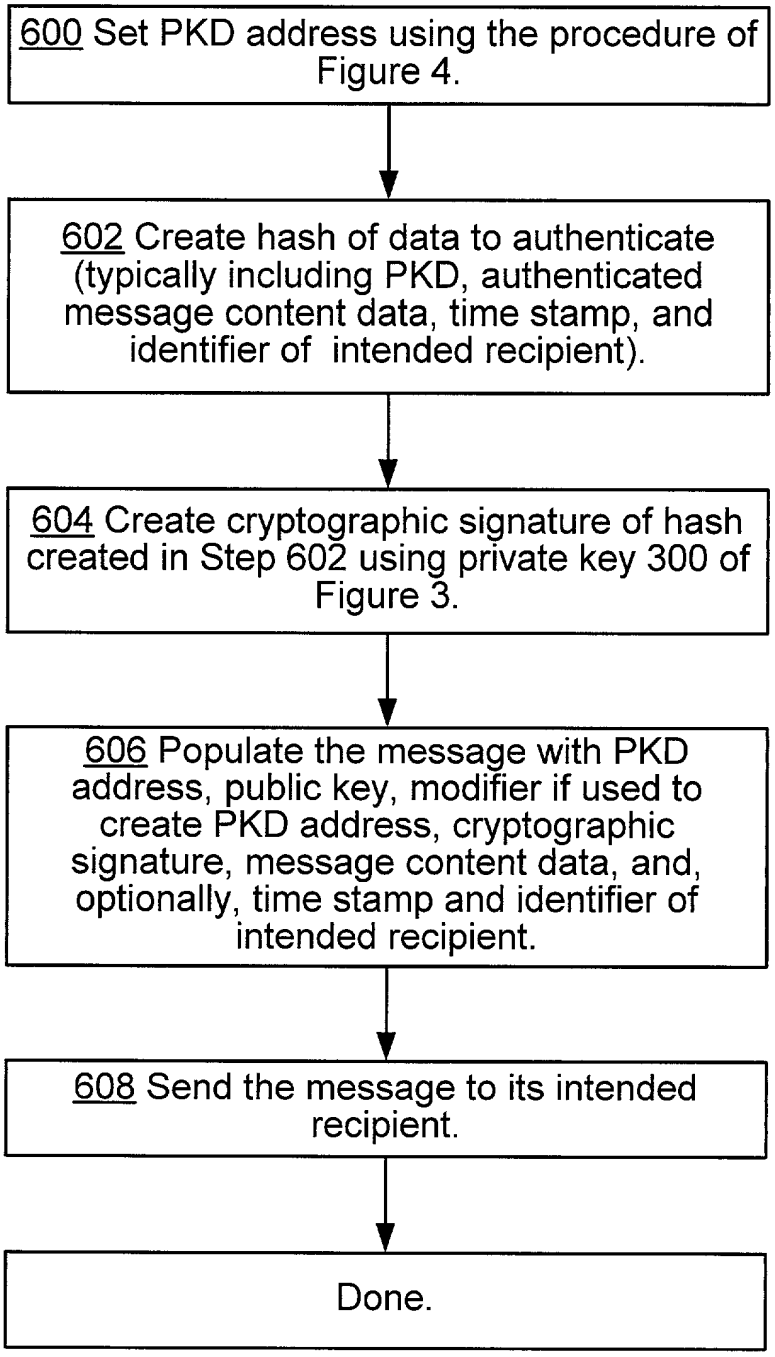

600 Set PKD address using the procedure of Figure 4.
602 Create hash of data to authenticate (typically including PKD, authenticated message content data, time stamp, and identifier of intended recipient).
604 Create cryptographic signature of hash created in Step 602 using private key 300 of Figure 3.
606 Populate the message with PKD address, public key, modifier if used to create PKD address, cryptographic signature, message content data, and, optionally, time stamp and identifier of intended recipient.
608 Send the message to its intended recipient.
Done.

FIG. 7

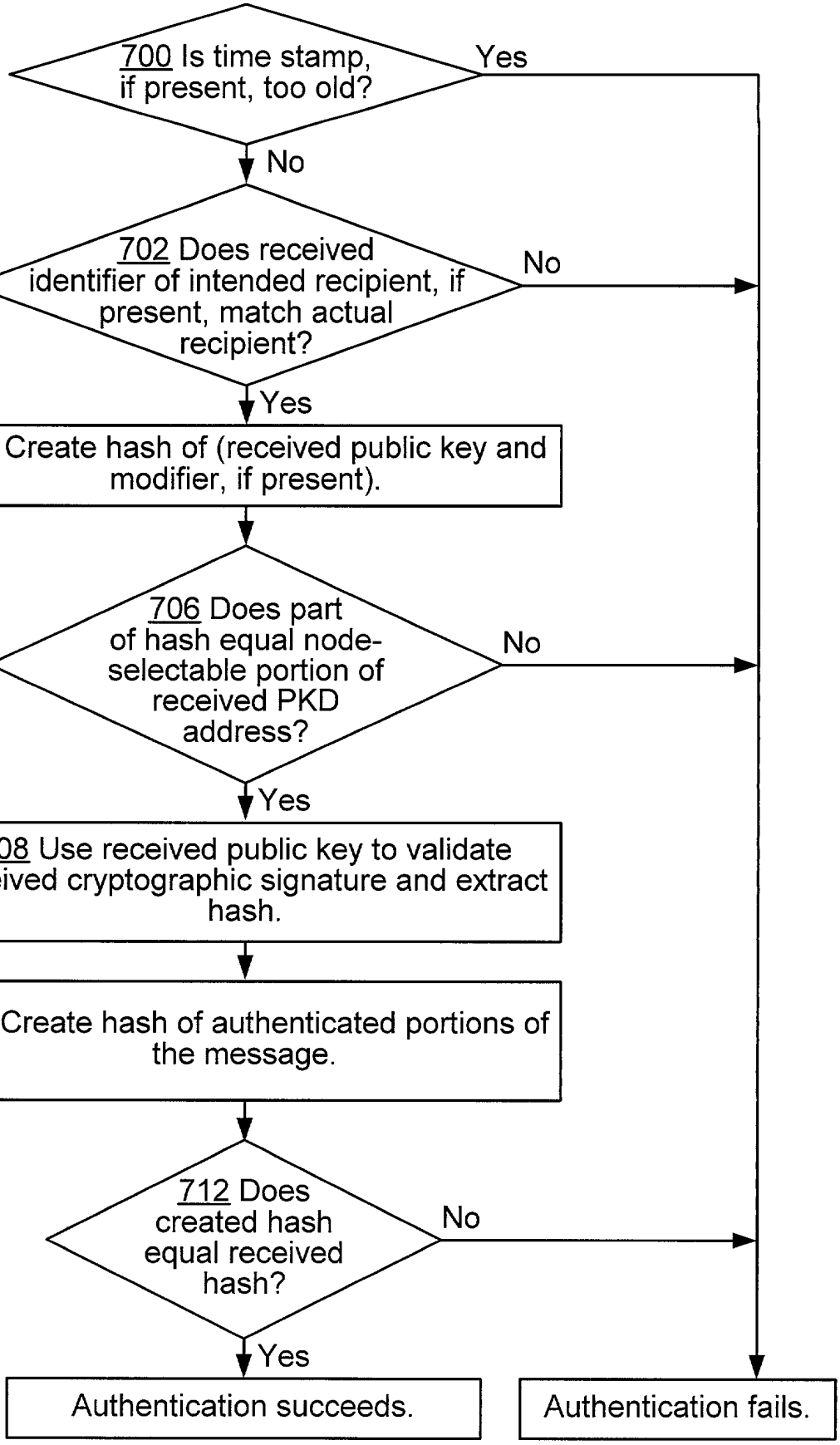

700 Is time stamp, if present, too old?
Yes
No
702 Does received identifier of intended recipient, if present, match actual recipient?
No
Yes
704 Create hash of (received public key and modifier, if present).
706 Does part of hash equal node-selectable portion of received PKD address?
No
Yes
708 Use received public key to validate received cryptographic signature and extract hash.
710 Create hash of authenticated portions of the message.
712 Does created hash equal received hash?
No
Yes
Authentication succeeds.
Authentication fails.

FIG. 8a

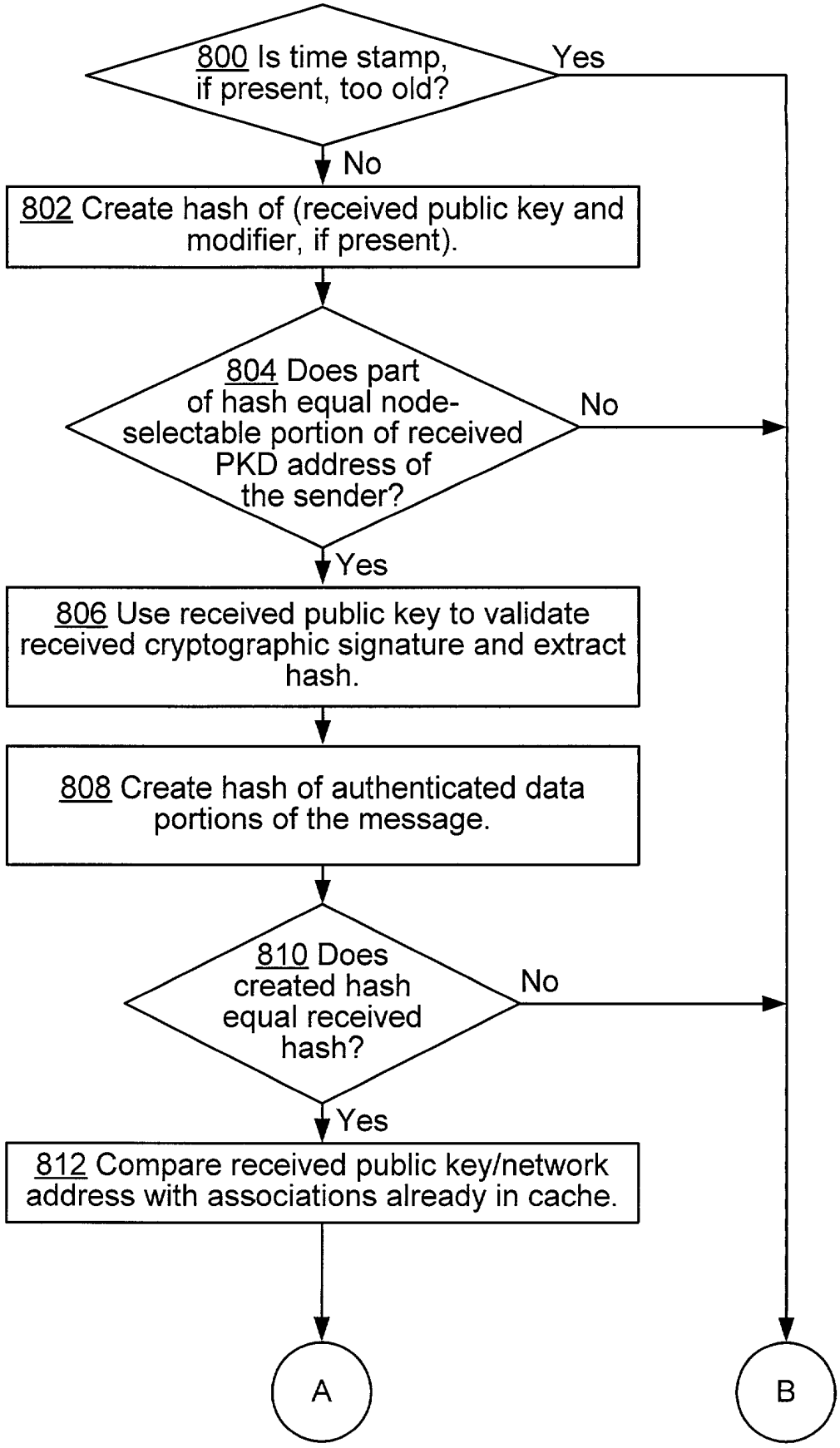

800 Is time stamp, if present, too old?
Yes
No
802 Create hash of (received public key and modifier, if present).
804 Does part of hash equal node-selectable portion of received PKD address of the sender?
No
Yes
806 Use received public key to validate received cryptographic signature and extract hash.
808 Create hash of authenticated data portions of the message.
810 Does created hash equal received hash?
No
Yes
812 Compare received public key/network address with associations already in cache.
A
B

FIG. 8b

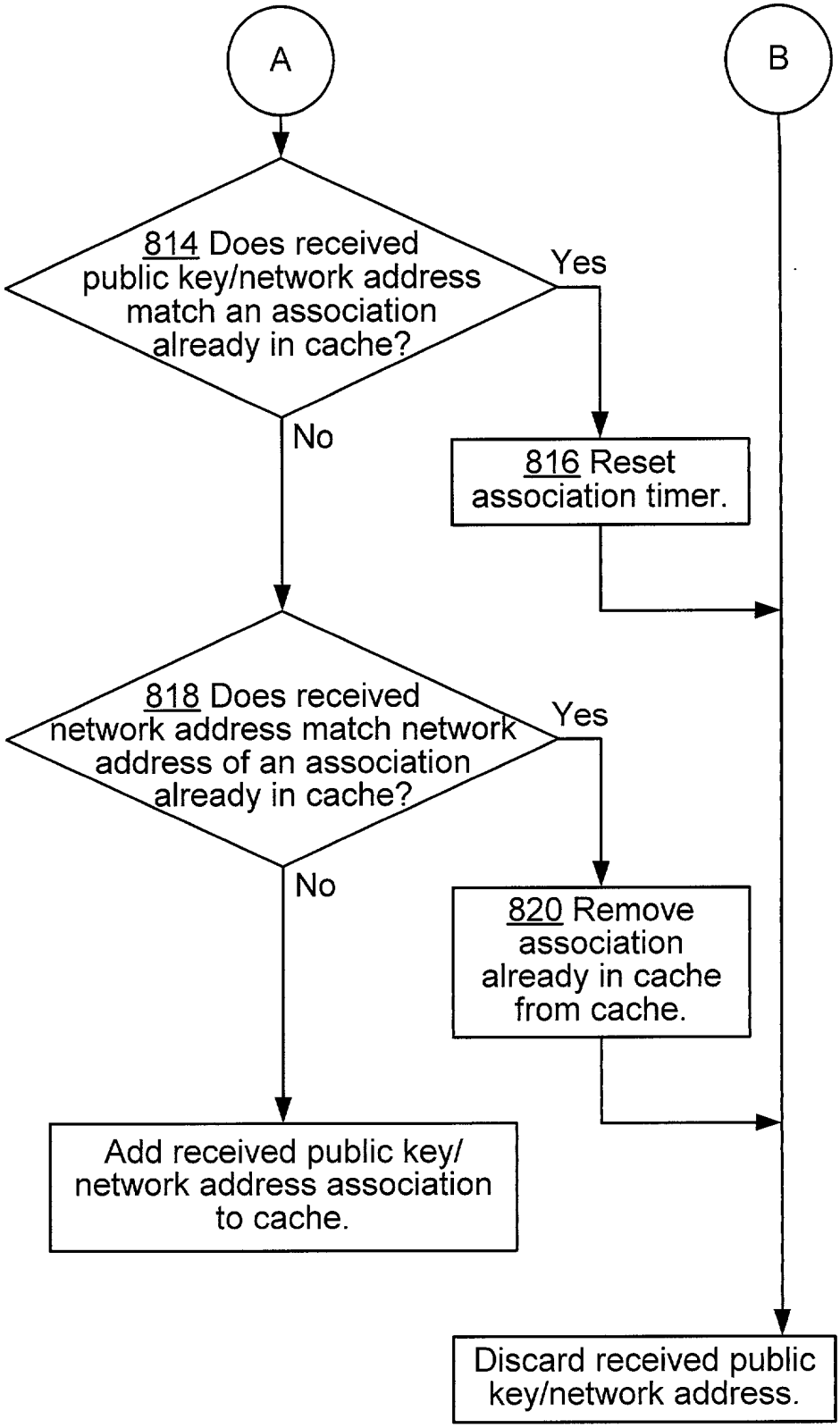
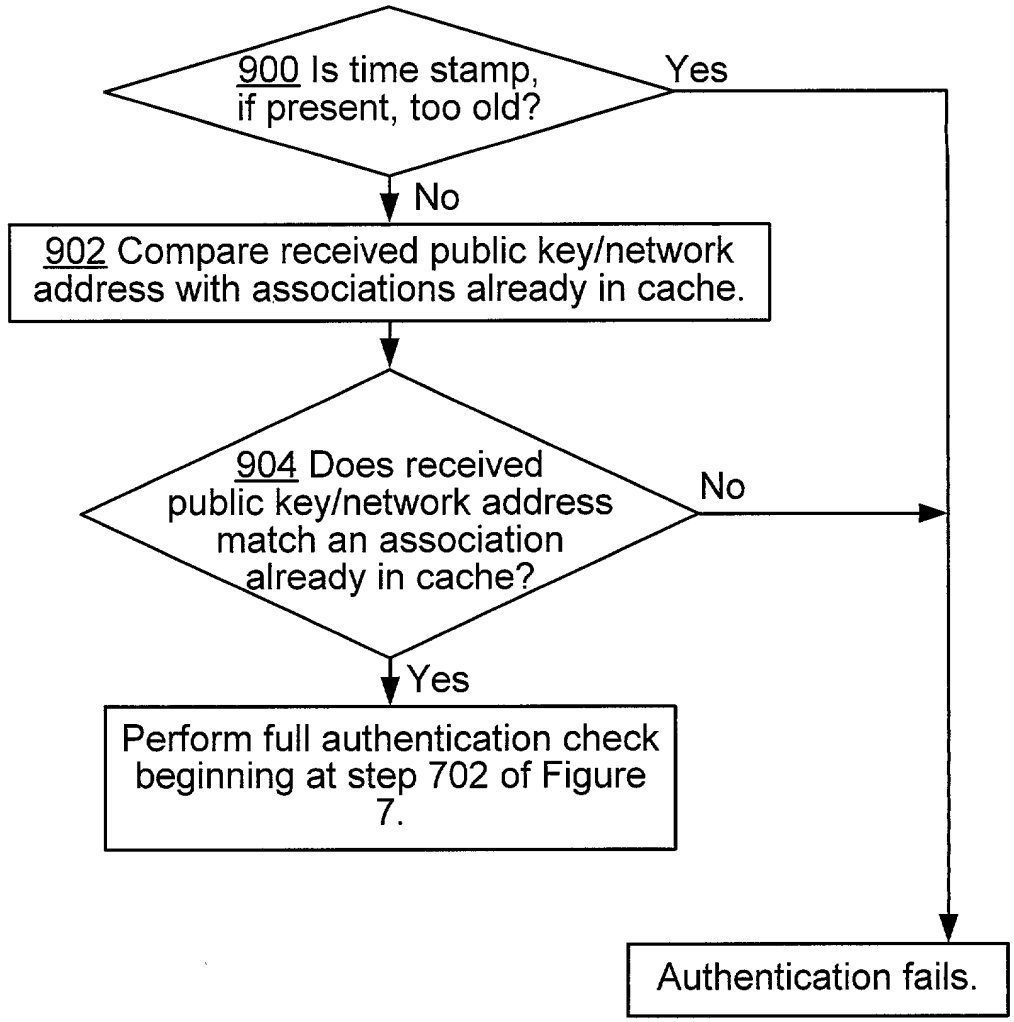

A
B
814 Does received public key/network address match an association already in cache?
Yes
No
816 Reset association timer.
818 Does received network address match network address of an association already in cache?
Yes
No
820 Remove association already in cache from cache.
Add received public key/ network address association to cache.
Discard received public key/network address.

FIG. 9


900 Is time stamp, if present, too old?
Yes
No
902 Compare received public key/network address with associations already in cache.
904 Does received public key/network address match an association already in cache?
No
Yes
Perform full authentication check beginning at step 702 of Figure 7.
Authentication fails.